Quantum eMotion Announces Launch and Availability of eShield-Q, a Runtime Cryptographic Protection Platform for the AI and Quantum Era

written by Raj Shah | May 4, 2026

May 4, 2026 (Source) – Quantum eMotion Corp. (NYSE American: QNC) (TSXV: QNC) (FSE: 34Q0) ("QeM" or the "Company"), a leader in quantum-secure cybersecurity solutions, is pleased to announce the launch and availability of eShield-Q, a new cybersecurity platform designed to address one of the fastest-growing risks in the digital economy: the exposure of cryptographic operations during application runtime.

As organizations scale AI infrastructure, cloud platforms, identity systems, digital services, and secure communications, the attack surface continues to expand. At the same time, advances in artificial intelligence and the approaching reality of quantum computing are accelerating the pace, scale, and sophistication of cyber threats. eShield-Q is built on the premise that securing cryptographic operations during execution is not an added defense, but a fundamental requirement for protecting modern systems.

eShield-Q introduces a dedicated runtime cryptographic protection layer designed to protect critical secrets, including encryption keys, entropy sources, deterministic random bit generator states, and cryptographic execution environments, even

under advanced attack conditions where memory, operating systems, kernels, or hypervisors may no longer be fully trusted. The platform reflects QeM's "assume compromise" security model, recognizing that modern cryptography must increasingly be protected while it is actively in use.

"Cybersecurity is entering a new phase where traditional protections alone are no longer enough," said Jason Thomas, Director of Product Development at Quantum eMotion. "The reality is that the most critical processes — cryptographic operations — remain exposed during execution. As AI-driven threats accelerate and quantum risks come into focus, securing these foundational processes is essential to protecting everything from AI infrastructure and identity systems to web services and the critical data and systems they support."

Protecting Cryptography Where It Is Most Exposed

Encryption protects data, but the cryptographic stack itself can remain vulnerable while keys are generated, stored, accessed, or used in memory. Attack vectors such as memory scraping, side-channel attacks, kernel compromise, remote code execution, hypervisor exploits, entropy degradation, and deterministic random bit generator state compromise can expose or corrupt the cryptographic processes on which secure systems depend.

Traditional cybersecurity approaches are often reactive, relying on patch cycles, vulnerability disclosure, perimeter defenses, or post-incident remediation. eShield-Q is designed to address this gap by protecting cryptographic operations at runtime — the point where keys, entropy, and algorithms are actively used.

"Security assumptions are changing quickly," said Dr. Francis Bellido, Chief Executive Officer of Quantum eMotion. "AI is accelerating vulnerability discovery and exploit generation, while quantum computing is reshaping the long-term security

requirements of modern cryptography. With eShield-Q, Quantum eMotion is addressing a critical missing layer in cybersecurity: protecting cryptography itself while it runs. More importantly, eShield-Q now completes and strengthens our broader product portfolio, allowing QeM to secure digital systems from cloud to chip – from cloud applications, AI pipelines, identity platforms, VPNs and secure communications, down to entropy generation, memory-secure keys, and future secure silicon architectures. By combining quantum entropy, post-quantum cryptography, SecureKey's memory-secure execution model, and hardened runtime protection, QeM is building an integrated platform designed to help organizations defend against today's AI-accelerated cyberattacks and prepare for tomorrow's quantum-computing threats."

Quantum Entropy, Memory-Secure Keys, and Runtime Assurance

The eShield-Q platform combines three core capabilities:

- Quantum entropy through eFlux-Q
- eShield-Q leverages Quantum eMotion's quantum entropy capabilities to support the generation of cryptographic keys from true quantum randomness, reducing reliance on predictable, degraded, or compromised entropy sources.
- Memory-secure cryptography through SecureKey

The platform incorporates memory-secure key protection techniques designed to reduce key exposure during use, including register-based protection for symmetric keys and just-in-time decryption for larger asymmetric keys and secrets.

Hardened runtime protection

eShield-Q is designed to provide continuous runtime validation of cryptographic operations, including integrity checks, key

monitoring, code validation, and safeguards across stack, heap, and CPU boundaries.

Together, these capabilities are intended to help organizations protect cryptography across the full lifecycle of execution — from key generation and entropy assurance to runtime integrity and memory-secure operation.

Designed for Seamless Integration into Existing Environments

eShield-Q is designed to integrate into existing environments without requiring major application rewrites. The platform supports OpenSSL-compatible deployment models, enabling organizations to strengthen security across critical applications and infrastructure while minimizing operational disruption.

Potential deployment environments include:

- AI systems and AI pipelines;
- Identity and authentication platforms;
- TLS termination, including NGINX and ingress systems;
- VPN and IPsec gateways;
- Databases such as PostgreSQL and MongoDB;
- Web services, secure communications, and cloud-native applications;
- Enterprise, government, and critical infrastructure environments.

By protecting cryptography at the point where it is actively used, eShield-Q establishes a new control point for securing data, systems, and applications in use.

Strategic Expansion of Quantum eMotion’s Cybersecurity Portfolio

The introduction of eShield-Q marks a strategic expansion of

Quantum eMotion’s cybersecurity portfolio, extending its capabilities beyond quantum entropy solutions into a broader platform designed to address the evolving needs of enterprise, government, cloud, AI, and digital infrastructure customers.

eShield-Q complements QeM’s existing quantum random number generation, entropy-as-a-service, post-quantum cryptographic integration, and SecureKey technologies. The Company believes this integrated approach establishes a foundational security layer for the AI era and positions Quantum eMotion to help define an emerging cybersecurity category focused on protecting cryptography in use.

Showcase at the Cybersecurity and Identity Summit

As part of the launch, Quantum eMotion will showcase eShield-Q at the Cybersecurity and Identity Summit, a leading cybersecurity conference. The Company’s session, “Runtime Cryptographic Protection for the AI Era,” will highlight why protecting cryptographic operations during execution is becoming essential as organizations face AI-enabled threats, and how Quantum eMotion’s integrated quantum random number generation and post-quantum cryptography capabilities can support quantum-resilient keys and next-generation secure systems.

Availability

eShield-Q is now available for customer demonstrations, partner integrations, and selected pilot deployments. Quantum eMotion will initially focus on enterprise, cloud, AI, digital asset, infrastructure, and government-related environments where the protection of cryptographic keys and runtime execution is critical.

About Quantum eMotion

Company's mission is to address the growing demand for affordable hardware and software security for connected devices. Thanks to its patented Quantum Random Number Generator, QeM has become a pioneering force in classical and quantum cybersecurity solutions. This security solution exploits quantum mechanics' built-in unpredictability and promises to provide enhanced protection for high-value assets and critical systems. For further information, please visit our website at https://www.quantumemotion.com/ or contact us at: info@quantumemotion.com.

The Company intends to target highly valued Financial Services, Healthcare, Blockchain Applications, Cloud-Based IT Security Infrastructure, Classified Government Krown Technologies and Communication Systems, Secure Device Keying (IOT, Automotive, Consumer Electronics) and Quantum Cryptography.

For further information, please visit our website at https://www.quantumemotion.com/ or contact:

Francis Bellido, Chief Executive Officer
Tel: 514.956.2525
Email: info@quantumemotion.com
Website: www.quantumemotion.com

Cautionary Note regarding Forward-Looking Statements

This news release contains "forward-looking information" within the meaning of applicable securities laws, which is based upon the Company's current internal expectations, estimates, projections, assumptions and beliefs. Such forward-looking statements and forward-looking information include, but are not limited to, statements concerning the Company's expectations with respect to the commencement of trading of the Company's common shares on NYSE American; the expected cessation of trading on the OTCQB; the anticipated benefits of the NYSE

American listing; and the Company's business strategy, target markets and growth initiatives. Forward-looking statements or forward-looking information relate to future events and future performance and include statements regarding the expectations and beliefs of management based on information currently available to the Company. Such forward-looking statements and forward-looking information often, but not always, can be identified by the use of words such as "plans", "expects", "potential", "is expected", "anticipated", "is targeted", "budget", "scheduled", "estimates", "forecasts", "intends", "anticipates", or "believes" or the negatives thereof or variations of such words and phrases or statements that certain actions, events or results "may", "could", "would", "might" or "will" be taken, occur or be achieved. Forward-looking statements or forward-looking information are subject to a variety of risks and uncertainties which could cause actual events or results to differ materially from those reflected in the forward-looking statements or forward-looking information, including, without limitation, risks and uncertainties relating to delays in or failure to complete listing-related processes, the Company's ability to maintain compliance with applicable exchange requirements, changes in market conditions,, the value of the Company's intangible assets, completing proof of concept studies, protecting intangible assets rights, timing and availability of external financing on acceptable terms or at all, the possibility that future results will not be consistent with the Company's expectations, increases in costs, changes in legislation and regulation, changes in economic and political conditions and other risks inherent to the cybersecurity industry and new technologies, such as risk of obsolescence, slow adoption and competing technological advances; and those risks set out in the Company's public documents filed on SEDAR+ at www.sedarplus.ca.

Should one or more of these risks and uncertainties materialize, or should underlying assumptions prove incorrect, actual results may vary materially from those described in forward-looking statements or forward-looking information. Although the Company has attempted to identify important factors that could cause actual results to differ materially, there may be other factors that could cause results not to be as anticipated, estimated or intended. For more information on the Company and the risks and challenges of its business, investors should review the Company's annual filings that are available at www.sedarplus.ca. The Company provides no assurance that forward-looking statements or forward-looking information will prove to be accurate, as actual results and future events could differ materially from those anticipated in such statements and information. Accordingly, readers should not place undue reliance on forward-looking statements and forward-looking information. Any forward-looking statement speaks only as of the date on which it is made and, except as may be required by applicable securities laws, the Company disclaims any intent or obligation to update any forward-looking information.

Neither TSX Venture Exchange nor its Regulation Services Provider (as that term is defined in the policies of the TSX Venture Exchange) accepts responsibility for the adequacy or accuracy of this release.